Exhibit Q

EXHIBIT C-1
Invalidity of U.S. Patent No. 9,198,042 in view of Aarnos

U.S. Patent Publication No. 2007/0288989 ("Aarnos") was published on December 13, 2007, and has an effective priority date of June 9, 2006 based on U.S. Patent Application No. 11/450,932, and therefore constitutes prior art under at least 35 U.S.C. §§ 102(a), (b), and/or (e) as to the Asserted Claims of U.S. Pat. No. 9,198,042 ("the '042 Patent"). Aarnos anticipates and/or renders obvious the Asserted Claims, either alone or in combination with one or more references identified in Defendants' Cover Pleading.

To the extent Plaintiff argues that Aarnos does not disclose any element below, a person of ordinary skill in the art would have found it obvious in view of Aarnos alone, with the knowledge of a person of ordinary skill in the art, and/or in view of the prior art systems and references disclosed in § II of Defendants' Invalidity Contentions and the exemplary citations and commentary provided for this claim in Exhibits C-1 to C-5 and Appendix C-C thereto. A person of ordinary skill in the art would have been motivated to combine and would have a reasonable expectation of success in combining these references because the cited references relate to the same technical field as Aarnos (i.e., network policy management).

The chart below provides representative examples of where each element is found within Aarnos. Citations are meant to be exemplary, not exhaustive, and Defendants reserve the right to identify and discuss additional portions of the reference in support of its contentions and/or to rebut arguments made by Plaintiff. Citations to figures, drawings, tables, and the like include reference to any accompanying or related text. All internal cross references are meant to incorporate the cross-referenced material as if fully set forth therein.

It is Defendants' position that Plaintiff's Disclosure of Asserted Claims and Infringement Contentions have not established that any accused product or service infringes any valid claim. Thus, Defendants' statements below should not be treated as an admission, implication, or suggestion that Defendants agree with Plaintiff regarding either the scope, construction, or interpretation of any of the Asserted Claims of the infringement theories advanced by Plaintiff in its Preliminary Infringement Contentions, including whether any Asserted Claims satisfies 35 U.S.C. §§ 101 OR 112. In certain cases, Defendants specify non-limiting examples of where its application of the prior art is based on Plaintiff's apparent application of the claim element. These statements are not intended to suggest that Defendants agree with Plaintiff's application of any claim term, suggest a proposed construction at this stage of the case, or suggest that construction is needed, as the parties are not required to exchange terms for construction or proposed constructions until a later date.

Plaintiff has yet to identify of the Asserted Claims that it contends is not anticipated and/or rendered obvious by Aarnos. Defendants therefore expressly reserve the right to respond to any such contention, including by identifying additional obviousness combinations, if Plaintiff makes any such contention.

Where Defendants state that Aarnos "discloses" a limitation, that disclosure may be express, implicit, and/or inherent.

U.S. Patent No. US 9,198,042 (the "'042 Patent")	
Claim Language	**Exemplary Disclosure**
[1p] A method comprising:	Aarnos discloses a method. *See, e.g.:* 1. A method of updating a security policy associated with an electronic device, said method comprising: Receiving a policy update script comprising one or more modifications to the security policy; and Processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 2. The method of claim 1, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received. 3. The method of claim 2 further comprising: Verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. 4. The method of claim 1 further comprising: Receiving a new software component associated with the policy update script; and Installing the new software component. 5. The method of claim 4, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. 6. The method of claim 5, wherein the modifications further grant one or more existing software components permission to access the new software component.

	12. The electronic device of claim 10, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device, and wherein the modifications further grant one or more existing software components permission to access the new software component. 13. An apparatus capable of updating a security policy associated with an electronic device, said apparatus comprising: A processor; and A memory in communication with the processor, said memory storying an application executable by the processor, wherein the application is configured, upon execution, to: Generate a policy update script comprising one or more modifications to the security policy, said policy update script capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and Transmit the policy update script. 19. A system for updating a security policy associated with an electronic device, said system comprising: an apparatus configured to generate a policy update script comprising one or more modifications to the security policy, said apparatus further configured to transmit the policy update script; and an electronic device configured to receive the policy update script, said electronic device comprising an OSGi policy update resource processor configured to process the policy update script received in order to effect the modifications to the security policy. 20. The system of claim 19, wherein the apparatus is further configured to associate a signature with the policy update script, such that transmitting the policy update script comprises transmitting the policy update script and the associated signature. 21. The system of claim 20, wherein the electronic device is further configured to verify the signature in order to determine whether a party associated with the apparatus is authorized to modify the security policy.

	22. The system of claim 19, wherein the apparatus is further configured to combine the policy update script with a new software component and to transmit the new software component with the policy update script to the electronic device. 23. The system of claim 22, wherein the electronic device is further configured to receive the new software component and to install the software component. 24. The system of claim 23, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. 25. The system of claim 24, wherein the modifications further grant one or more existing software components permission to access the new software component. 26. The system of claim 22, wherein the apparatus is further configured to generate the new software component. 27. A computer program product for updating a security policy associated with an electronic device, wherein the computer program product comprises at least one computer-readable storage medium having computer-readable program code portions stored therein, said computer-readable program code portions comprising: a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 28. The computer program product of claim 27, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received. 29. The computer program product of claim 28, wherein the computer-readable program code portions further comprise: a third executable portion for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy.

	30. The computer program product of claim 27, wherein the computer-readable program code portions further comprise: a third executable portion for receiving a new software component associated with the policy update script; and a fourth executable portion for installing the new software component. 31. The computer program product of claim 30, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. 32. The computer program product of claim 31, wherein the modifications further grant one or more existing software components permission to access the new software component. 33. An apparatus for updating a security policy associated with an electronic device, said apparatus comprising: a means for receiving a policy update script comprising one or more modifications to the security policy; and a means for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 34. The apparatus of claim 33, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received, said apparatus further comprising: a means for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. 35. The apparatus of claim 33 further comprising: a means for receiving a new software component associated with the policy update script; and

	a means for installing the new software component, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device and one or more existing software components permission to access the new software component. **[0010]** In accordance with one aspect, a method is provided of updating a security policy associated with an electronic device. In one exemplary embodiment, the method includes: (1) receiving a policy update script comprising one or more modifications to the security policy; and (2) processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0011]** According to another aspect, an electronic device is provided that is capable of updating a security policy associated with the electronic device. In one exemplary embodiment the electronic device includes an OSGi policy update resource processor that is configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **[0012]** According to yet another aspect, an apparatus is provided that is capable of updating a security policy associated with an electronic device. In one exemplary embodiment, the apparatus includes a processor and a memory in communication with the processor that stores an application executable by the processor, wherein the application is configured, upon execution, to: (1) generate a policy update script comprising one or more modifications to the security policy, wherein the policy update script is capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and (2) transmit the policy update script. **[0013]** In accordance with another aspect, a system is provided for updating a security policy associated with an electronic device. In one exemplary embodiment, the system includes: (1) a network entity configured to generate a policy update script comprising one or more modifications to the security policy and to transmit the policy update script; and (2) an electronic device configured to receive the policy update script, wherein the electronic device comprises an OSGi policy update resource processor that is configured to process the policy update script received in order to effect the modifications to the security policy. **[0014]** In accordance with yet another aspect, a computer program product is provided for updating a security policy associated with an electronic device. The computer program product contains at least one computer-readable storage medium having computer-readable program code portions stored

	therein. The computer-readable program code portions of one exemplary embodiment include: (1) a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and (2) a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0021]** Reference is now made to **FIG. 1**, which illustrates the steps which may be taken in order to update the security policy associated with a particular electronic device (e.g., cellular telephone, PDA, PC, laptop, pager, television, or one or more electronic devices operating on a motor vehicle.). As shown, in one exemplary embodiment, the process may begin when a party, such as a software developer, creates or develops a software component or application to be installed on the electronic device. (Step **101**). As discussed above, software components are applications operating on an electronic device that may provide services to other components on the device and are likewise capable of dynamically discovering and using services of those other software components and applications. As is discussed in more detail below, Step **101** is optional. In other words exemplary embodiments of the present invention are not limited to instances where new software components are being developed for deployment on electronic devices. **[0022]** Once the software component has been developed, in Step **102**, a policy update script is generated that describes the modifications that must be made to the electronic device security policy in order to enable the new software component to access other services and resources of the electronic device, and vice versa (i.e., the modifications grant the appropriate permissions to the various components). The policy update script may, for example, be in the form of an Extensible Markup Language (XML) file, or the like. **[0023]** The developed software component and the corresponding policy update script are then combined, in Step **103** into a deployment (or installation) package for deployment on the device. The deployer (or party responsible for creating the deployment package and providing it to the electronic device, which may or may not be the software developer), in Step **104** signs the package (i.e., incorporates a digital signature, such as a private key, with the package). The signature will be used to verify whether and to what extent the signer (i.e., the deployer) is authorized to modify the electronic device security policy; thus providing increased security to the policy updating process. In one exemplary embodiment, different parties may be provided with different levels of authorization. For example, where one party may have authorization to make wholesale modifications to the existing security policy, other parties may have only restricted access.

	[0024] The deployment or installation package, including the software component, the policy update script and the signature, is then provided to the device in Step **105**. In one exemplary embodiment, this step is performed where the user of the electronic device initiates the download of the software component over a network, such as a wide area network (WAN), or the like. Alternatively, the software component may be pushed to the electronic device. As one of ordinary skill in the art will recognize, the software component may be transmitted via any number of mechanisms, including, for example, over Bluetooth, a USB cable, infrared, or even a multimedia card (MMC), without departing from the spirit and scope of exemplary embodiments of the present invention. **[0025]** Regardless of how the deployment package is received by the electronic device (in Step **106**), upon receipt, installation of the deployment package begins (Step **107**). In one exemplary embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment package is in fact authorized to modify the existing security policy of the mobile device (Step 108). Assuming the signature is verified and that the deployer is authorized (based on the existing electronic device security policy), in Step **109**, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script. **[0026]** In particular, according to the OSGi specification, a deployment service exists on the electronic device that is configured to process deployment or installation packages received by the electronic device. This deployment service comprises one or more plug-ins called resource processors, wherein different resource processors are capable of processing different installation packages. In particular, resource processors, or software components that may be located on the device itself or within the deployment package to be installed, handle the lifecycle of specific resource types by processing the resource to create artifacts that are then removed when the resource is dropped. The use of a plug-in architecture for the deployment service is beneficial since it enables the use of multiple types of resources in the installation package (i.e., for each new type of resource a new resource processor, or plug-in, can be added where necessary). **[0027]** According to exemplary embodiments of the present invention, a new plug-in or OSGi resource processor, referred to as the Policy Update Resource Processor is included in the deployment service. The Policy Update Resource Processor is configured to recognize the policy update script and to conduct the necessary security policy update according to the script. In one exemplary embodiment, usage of the Policy Update Resource Processor is protected by a new Java 2 permission, such that only deployment packages assigned this new permission can run this new processor. The assignment of the Java 2 permission is carried out based on the signature information of the deployment package.

	In other words, verifying the signature incorporated with the package in order to determine whether, and to what extent, the signer is authorized to modify the security policy, in essence verifies that the party signing the package has been given the new permission. **[0031]** For example, one method of granting the requisite permissions is based on the creation of different developer platforms, wherein a special developer certificate may be locked to the IMEIs of one or more specific devices. Developers use private keys corresponding to these certificates when signing their applications. The applications can then be executed on the devices with the listed IMEIs. One drawback to this method, however, is that it assumes that the root certificates that can be used for signing the developer certificates have been provided to the one or more devices at the time of manufacture. In addition, a special mechanism is required that can recognize that the developer certificate is locked to particular IMEI numbers and act accordingly. **[0049]** The system, method, electronic device, network entity and computer program product of exemplary embodiments of the invention are primarily described in conjunction with mobile communications applications. It should be understood, however, that the system, method, electronic device, network entity and computer program product of embodiments of the invention can be utilized in conjunction with a variety of other applications, both in the mobile communications industries and outside of the mobile communications industries. For example, the system, method, electronic device, network entity and computer program product of exemplary embodiments of the invention can be utilized in conjunction with wireline and/or wireless network (e.g., Internet) applications. **[0050]** As described above and as will be appreciated by one skilled in the art, embodiments of the invention may be configured as a system, method, electronic device, network entity and computer program product. Accordingly, embodiments of the invention may be comprised of various means including entirely of hardware, entirely of software, or any combination of software and hardware. Furthermore, embodiments of the invention may take the form of a computer program product on a computer-readable storage medium having computer-readable program instructions (e.g., computer software) embodied in the storage medium. Any suitable computer-readable storage medium may be utilized including hard disks, CD-ROMs, optical storage devices, or magnetic storage devices. **[0051]** Exemplary embodiments of the invention have been described above with reference to block diagrams and flowchart illustrations of methods, apparatuses (i.e., systems) and computer program products. It will be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by various means including computer program instructions. These computer program

	instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create a means for implementing the functions specified in the flowchart block or blocks. **Aarnos Fig. 1** To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1a] receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;	Aarnos discloses receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state. *See, e.g.:* 1. A method of updating a security policy associated with an electronic device, said method comprising: Receiving a policy update script comprising one or more modifications to the security policy; and Processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 2. The method of claim 1, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received. 3. The method of claim 2 further comprising: Verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. 4. The method of claim 1 further comprising: Receiving a new software component associated with the policy update script; and

	Installing the new software component. **7**. An electronic device capable of updating a security policy associated with the electronic device, said electronic device comprising: an OSGi policy update resource processor configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **8**. The electronic device of claim 7, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received. **9**. The electronic device of claim 8, wherein the resource processor is further configured to verify the signature in order to determine whether the transmitting party is authorized to modify the security policy. 11. The electronic device of claim 7 further comprising: a means to receive a new software component associated with the policy update script; and a means to install the new software component on the electronic device. 19. A system for updating a security policy associated with an electronic device, said system comprising: an apparatus configured to generate a policy update script comprising one or more modifications to the security policy, said apparatus further configured to transmit the policy update script; and an electronic device configured to receive the policy update script, said electronic device comprising an OSGi policy update resource processor configured to process the policy update script received in order to effect the modifications to the security policy. 27. A computer program product for updating a security policy associated with an electronic device, wherein the computer program product comprises at least one computer-readable storage medium

	having computer-readable program code portions stored therein, said computer-readable program code portions comprising: a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 33. An apparatus for updating a security policy associated with an electronic device, said apparatus comprising: a means for receiving a policy update script comprising one or more modifications to the security policy; and a means for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 34. The apparatus of claim 33, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received, said apparatus further comprising: a means for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. 35. The apparatus of claim 33 further comprising: a means for receiving a new software component associated with the policy update script; and a means for installing the new software component, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device and one or more existing software components permission to access the new software component. **[0010]** In accordance with one aspect, a method is provided of updating a security policy associated with an electronic device. In one exemplary embodiment, the method includes: (1) receiving a policy

	update script comprising one or more modifications to the security policy; and (2) processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0011]** According to another aspect, an electronic device is provided that is capable of updating a security policy associated with the electronic device. In one exemplary embodiment the electronic device includes an OSGi policy update resource processor that is configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **[0013]** In accordance with another aspect, a system is provided for updating a security policy associated with an electronic device. In one exemplary embodiment, the system includes: (1) a network entity configured to generate a policy update script comprising one or more modifications to the security policy and to transmit the policy update script; and (2) an electronic device configured to receive the policy update script, wherein the electronic device comprises an OSGi policy update resource processor that is configured to process the policy update script received in order to effect the modifications to the security policy. **[0014]** In accordance with yet another aspect, a computer program product is provided for updating a security policy associated with an electronic device. The computer program product contains at least one computer-readable storage medium having computer-readable program code portions stored therein. The computer-readable program code portions of one exemplary embodiment include: (1) a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and (2) a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0025]** Regardless of how the deployment package is received by the electronic device (in Step **106**), upon receipt, installation of the deployment package begins (Step **107**). In one exemplary embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment package is in fact authorized to modify the existing security policy of the mobile device (Step **108**). Assuming the signature is verified and that the deployer is authorized (based on the existing electronic device security policy), in Step **109**, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script.

	[0026] In particular, according to the OSGi specification, a deployment service exists on the electronic device that is configured to process deployment or installation packages received by the electronic device. This deployment service comprises one or more plug-ins called resource processors, wherein different resource processors are capable of processing different installation packages. In particular, resource processors, or software components that may be located on the device itself or within the deployment package to be installed, handle the lifecycle of specific resource types by processing the resource to create artifacts that are then removed when the resource is dropped. The use of a plug-in architecture for the deployment service is beneficial since it enables the use of multiple types of resources in the installation package (i.e., for each new type of resource a new resource processor, or plug-in, can be added where necessary). **[0034]** In particular, according to exemplary embodiments of the present invention, a developer may provide the IMEIs of the devices they would like to use as developer devices to an authorized policy administrator of those devices (i.e., to a party with authorization to create policy update scripts that will be read by a Policy Update Resource Processor on the device in order to modify the existing security policy). The authorized policy administrator, in turn, creates a policy update script granting the requisite permissions (e.g., AllPermission) to the developers and includes the IMEICondition in the script. In other words, the permission is granted conditionally only for those devices identified by their IMEI. The authorized policy administrator puts the script into a deployment package (i.e., the standard installation scripts of the OSGi platform), signs the package with his private key and then returns the signed package to the developer. Upon receipt of the package, the developer can execute the package on the device, which, in turn, executes the policy update script. The execution of the deployment package is authorized, based on the authorized policy administrator's signature, to perform the policy update script. From that point on, the developer will have all of the rights described in the policy update script, with respect to the device(s) identified by their IMEIs. If the deployment package were to be executed with respect to a device not identified in the IMEICondition, the device's security policy would not be affected, since the condition would not be met and, therefore, the permission would not be granted. **[0036]** Referring to **FIG. 2**, an illustration of one type of system that would benefit from exemplary embodiments of the present invention is provided. As shown in **FIG. 2**, the system can include one or more mobile stations **10**, each having an antenna 12 for transmitting signals to and for receiving signals from one or more base stations (BS's) **14**. The base station is a part of one or more cellular or mobile networks that each includes elements required to operate the network, such as one or more mobile switching centers (MSC) **16**. As well known to those skilled in the art, the mobile network may also be referred to as a Base Station/MSC/Interworking function (BMI). In operation, the MSC is

	capable of routing calls, data or the like to and from mobile stations when those mobile stations are making and receiving calls, data or the like. The MSC can also provide a connection to landline trunks when mobile stations are involved in a call. **[0040]** One or more mobile stations **10** (as well as one or more processing elements, although not shown as such in **FIG. 2**) can further be coupled to one or more wireless access points (APs) **36**. The AP's can be configured to communicate with the mobile station in accordance with techniques such as, for example, radio frequency (RF), Bluetooth (BT), infrared (IrDA) or any of a number of different wireless networking techniques, including WLAN techniques. The APs may be coupled to the Internet **20**. Like with the MSC **16**, the AP's can be directly coupled to the Internet. In one embodiment, however, the APs are indirectly coupled to the Internet via a GTW **28**. As will be appreciated, by directly or indirectly connecting the mobile stations and the processing elements (e.g., devices associated with the Authorized Policy Administrator **22** and/or Software Developer **24**) and/or any of a number of other devices to the Internet, whether via the AP's or the mobile network(s), the mobile stations and processing elements can communicate with one another to thereby carry out various functions of the respective entities, such as to transmit and/or receive data, content or the like. As used herein, the terms “data,” “content,” “information,” and similar terms may be used interchangeably to refer to data capable of being transmitted, received and/or stored in accordance with embodiments of the invention. Thus, use of any such terms should not be taken to limit the spirit and scope of embodiments of the invention. **[0043]** In addition to the memory **220**, the processor **210** can also be connected to at least one interface or other means for displaying, transmitting and/or receiving data, content or the like (e.g., for transmitting and/or receiving a generated software component, policy update script and/or signature). In this regard, the interface(s) can include at least one communication interface **230** or other means for transmitting and/or receiving data, content or the like, as well as at least one user interface that can include a display **240** and/or a user input interface **250**. The user input interface, in turn, can comprise any of a number of devices allowing the entity to receive data from a user, such as a keypad, a touch display, a joystick or other input device. **[0045]** The mobile station includes various means for performing one or more functions in accordance with exemplary embodiments of the invention, including those more particularly shown and described herein. It should be understood, however, that one or more of the entities may include alternative means for performing one or more like functions, without departing from the spirit and scope of embodiments of the invention. More particularly, for example, as shown in **FIG. 3,** in addition to an antenna **302**, the mobile station **10** includes a transmitter **304**, a receiver **306**, and means, such as a

	processing device **308**, e.g., a processor, controller or the like, that provides signals to and receives signals from the transmitter **304** and receiver **306**, respectively. These signals include signaling information in accordance with the air interface standard of the applicable cellular system and also user speech and/or user generated data. In this regard, the mobile station can be capable of operating with one or more air interface standards, communication protocols, modulation types, and access types. More particularly, the mobile station can be capable of operating in accordance with any of a number of second-generation (2G), 2.5G and/or third-generation (3G) communication protocols or the like. Further, for example, the mobile station can be capable of operating in accordance with any of a number of different wireless networking techniques, including Bluetooth, IEEE 802.11 WLAN (or Wi-Fi®), IEEE 802.16 WiMAX, ultra wideband (UWB), and the like. **[0047]** The mobile station may also comprise means such as a user interface including, for example, a conventional earphone or speaker **310**, a ringer **312**, a microphone **314**, a display **316**, all of which are coupled to the controller **308**. The user input interface, which allows the mobile device to receive data, can comprise any of a number of devices allowing the mobile device to receive data, such as a keypad **318**, a touch display (not shown), a microphone **314**, or other input device. In embodiments including a keypad, the keypad can include the conventional numeric (0-9) and related keys (#, *), and other keys used for operating the mobile station and may include a full set of alphanumeric keys or set of keys that may be activated to provide a full set of alphanumeric keys. Although not shown, the mobile station may include a battery, such as a vibrating battery pack, for powering the various circuits that are required to operate the mobile station, as well as optionally providing mechanical vibration as a detectable output. **Aarnos Figs. 1, 2.** To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1b] determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified, the particular service policy setting being stored in a protected partition of the wireless end-	Aarnos discloses determining, based on the report, that a particularly service policy setting of the wireless end-user device needs to be modified, [the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting,] the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting

user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting, the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and	configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network. *See, e.g.:* **1**. A method of updating a security policy associated with an electronic device, said method comprising: Receiving a policy update script comprising one or more modifications to the security policy; and Processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **2**. The method of claim 1, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received. **3**. The method of claim 2 further comprising: Verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. **5**. The method of claim 4, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. **6**. The method of claim 5, wherein the modifications further grant one or more existing software components permission to access the new software component. **7**. An electronic device capable of updating a security policy associated with the electronic device, said electronic device comprising: an OSGi policy update resource processor configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy.

	9. The electronic device of claim 8, wherein the resource processor is further configured to verify the signature in order to determine whether the transmitting party is authorized to modify the security policy. **10**. The electronic device of claim 9, wherein the resource processor is further configured to determine, based at least in part on the signature, an extent to which the transmitting party is authorized to modify the security policy. **12**. The electronic device of claim 10, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device, and wherein the modifications further grant one or more existing software components permission to access the new software component. **13**. An apparatus capable of updating a security policy associated with an electronic device, said apparatus comprising: a processor; and a memory in communication with the processor, said memory storing an application executable by the processor, wherein the application is configured, upon execution, to: generate a policy update script comprising one or more modifications to the security policy, said policy update script capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and transmit the policy update script. **14**. The apparatus of claim 13, wherein the application is further configured, upon execution, to associate a signature with the policy update script, said signature capable of being verified in order to determine whether a party associated with the apparatus is authorized to modify the security policy. **16**. The apparatus of claim 15, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device.

	17. The apparatus of claim 16, wherein the modifications further grant one or more existing software components permission to access the new software component. **19**. A system for updating a security policy associated with an electronic device, said system comprising: an apparatus configured to generate a policy update script comprising one or more modifications to the security policy, said apparatus further configured to transmit the policy update script; and an electronic device configured to receive the policy update script, said electronic device comprising an OSGi policy update resource processor configured to process the policy update script received in order to effect the modifications to the security policy. **21**. The system of claim 20, wherein the electronic device is further configured to verify the signature in order to determine whether a party associated with the apparatus is authorized to modify the security policy. **24**. The system of claim 23, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. **25**. The system of claim 24, wherein the modifications further grant one or more existing software components permission to access the new software component. **27**. A computer program product for updating a security policy associated with an electronic device, wherein the computer program product comprises at least one computer-readable storage medium having computer-readable program code portions stored therein, said computer-readable program code portions comprising: a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy.

	29. The computer program product of claim 28, wherein the computer-readable program code portions further comprise: a third executable portion for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. **31**. The computer program product of claim 30, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. **32**. The computer program product of claim 31, wherein the modifications further grant one or more existing software components permission to access the new software component. **33**. An apparatus for updating a security policy associated with an electronic device, said apparatus comprising: a means for receiving a policy update script comprising one or more modifications to the security policy; and a means for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **34**. The apparatus of claim 33, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received, said apparatus further comprising: a means for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. **35**. The apparatus of claim 33 further comprising: a means for receiving a new software component associated with the policy update script; and a means for installing the new software component, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications

	installed on the electronic device and one or more existing software components permission to access the new software component. **[0006]** Other situations may similarly exist where it would be desirable for parties other than the manufacture or network operator, to be able to modify the existing security policy of the electronic device (i.e., in addition to where a new software component is introduced). For example, a software developer may desire to change the security policy on one or more electronic devices in order to test various applications he or she is developing. In addition, companies that provide their employees with mobile devices (e.g., cell phones and/or PDAs) may have specific software that can only be run on that company's devices and require special permissions within the device. It may be desirable for the company to be able to install the necessary rights to the mobile device at the same time the software is being installed. **[0007]** Currently, however, in order to modify the electronic device security policy, a party must have AllPermission, a Java-based permission that grants permission to access everything on the electronic device, or a similar and equally powerful permission. However, manufacturers and, in some instances, network operators are generally the only parties with such a powerful permission. This makes it nearly impossible for any party other than the manufacturer or network operator to modify the existing security policy. **[0008]** A need, therefore, exists for a way for parties not limited to the device manufacturer or network operator to modify the existing security policy of an electronic device after a user has taken possession of the electronic device. **[0009]** In general, exemplary embodiments of the present invention provide an improvement over the known prior art by, among other things, providing a convenient and safe way to update the security policy associated with an electronic device, such as a cellular telephone, personal digital assistant (PDA), personal computer (PC), laptop, pager, television, or the like, or one or more electronic devices operating on a motor vehicle, after a user has purchased the device and taken it away for use. In particular, exemplary embodiments provide a scripting tool that can be used to create a policy update script, or resource application or file, that describes the desired modifications to an electronic device security policy. Exemplary embodiments further provide an OSGi resource processor, referred to as a Policy Update Resource Processor, that is located on the electronic device and is configured to carry out the security policy modifications outlined in the policy update script. In particular, in one exemplary embodiment, the modifications may be those necessary to provide a new software component, with which the script corresponds, the requisite permissions to access other software

	components and resources available on the electronic device. The script may also describe how the security policy should be modified, in turn, to provide the other software components access to the services of the new software component. **[0010]** In accordance with one aspect, a method is provided of updating a security policy associated with an electronic device. In one exemplary embodiment, the method includes: (1) receiving a policy update script comprising one or more modifications to the security policy; and (2) processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0011]** According to another aspect, an electronic device is provided that is capable of updating a security policy associated with the electronic device. In one exemplary embodiment the electronic device includes an OSGi policy update resource processor that is configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **[0012]** According to yet another aspect, an apparatus is provided that is capable of updating a security policy associated with an electronic device. In one exemplary embodiment, the apparatus includes a processor and a memory in communication with the processor that stores an application executable by the processor, wherein the application is configured, upon execution, to: (1) generate a policy update script comprising one or more modifications to the security policy, wherein the policy update script is capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and (2) transmit the policy update script. **[0013]** In accordance with another aspect, a system is provided for updating a security policy associated with an electronic device. In one exemplary embodiment, the system includes: (1) a network entity configured to generate a policy update script comprising one or more modifications to the security policy and to transmit the policy update script; and (2) an electronic device configured to receive the policy update script, wherein the electronic device comprises an OSGi policy update resource processor that is configured to process the policy update script received in order to effect the modifications to the security policy. **[0014]** In accordance with yet another aspect, a computer program product is provided for updating a security policy associated with an electronic device. The computer program product contains at least one computer-readable storage medium having computer-readable program code portions stored therein. The computer-readable program code portions of one exemplary embodiment include: (1) a

	first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and (2) a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0021]** Reference is now made to **FIG. 1**, which illustrates the steps which may be taken in order to update the security policy associated with a particular electronic device (e.g., cellular telephone, PDA, PC, laptop, pager, television, or one or more electronic devices operating on a motor vehicle.). As shown, in one exemplary embodiment, the process may begin when a party, such as a software developer, creates or develops a software component or application to be installed on the electronic device. (Step **101**). As discussed above, software components are applications operating on an electronic device that may provide services to other components on the device and are likewise capable of dynamically discovering and using services of those other software components and applications. As is discussed in more detail below, Step **101** is optional. In other words exemplary embodiments of the present invention are not limited to instances where new software components are being developed for deployment on electronic devices. **[0022]** Once the software component has been developed, in Step **102**, a policy update script is generated that describes the modifications that must be made to the electronic device security policy in order to enable the new software component to access other services and resources of the electronic device, and vice versa (i.e., the modifications grant the appropriate permissions to the various components). The policy update script may, for example, be in the form of an Extensible Markup Language (XML) file, or the like. **[0023]** The developed software component and the corresponding policy update script are then combined, in Step **103** into a deployment (or installation) package for deployment on the device. The deployer (or party responsible for creating the deployment package and providing it to the electronic device, which may or may not be the software developer), in Step **104** signs the package (i.e., incorporates a digital signature, such as a private key, with the package). The signature will be used to verify whether and to what extent the signer (i.e., the deployer) is authorized to modify the electronic device security policy; thus providing increased security to the policy updating process. In one exemplary embodiment, different parties may be provided with different levels of authorization. For example, where one party may have authorization to make wholesale modifications to the existing security policy, other parties may have only restricted access. **[0025]** Regardless of how the deployment package is received by the electronic device (in Step **106**), upon receipt, installation of the deployment package begins (Step **107**). In one exemplary

	embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment package is in fact authorized to modify the existing security policy of the mobile device (Step **108**). Assuming the signature is verified and that the deployer is authorized (based on the existing electronic device security policy), in Step **109**, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script. **[0027]** According to exemplary embodiments of the present invention, a new plug-in or OSGi resource processor, referred to as the Policy Update Resource Processor is included in the deployment service. The Policy Update Resource Processor is configured to recognize the policy update script and to conduct the necessary security policy update according to the script. In one exemplary embodiment, usage of the Policy Update Resource Processor is protected by a new Java 2 permission, such that only deployment packages assigned this new permission can run this new processor. The assignment of the Java 2 permission is carried out based on the signature information of the deployment package. In other words, verifying the signature incorporated with the package in order to determine whether, and to what extent, the signer is authorized to modify the security policy, in essence verifies that the party signing the package has been given the new permission. **[0028]** As mentioned briefly above, exemplary embodiments of the present invention are not limited to situations where a new software component is to be installed on the electronic device. In contrast, the policy update script may be used any time a party desires to modify the existing security policy and is authorized to do so. In one exemplary embodiment, rather than including the policy update script in a deployment package for a new software component, a manufacturer or operator may create an "empty" deployment or installation package containing only the policy update script (thus eliminating Step **101**). The manufacturer or operator could then provide the package to the appropriate parties, such as the software developer. Using this technique, manufacturers and operators would no longer be required to run the actual installation or remote policy management themselves. The below exemplary use case provides an example of where an empty deployment package may be used. **[0048]** The mobile station can also include means, such as memory including, for example, a subscriber identity module (SIM) **320**, a removable user identity module (R-UIM) (not shown), or the like, which typically stores information elements related to a mobile subscriber. In addition to the SIM, the mobile device can include other memory. In this regard, the mobile station can include volatile memory **322**, as well as other non-volatile memory **324**, which can be embedded and/or may be removable. For example, the other non-volatile memory may be embedded or removable multimedia memory cards (MMCs), Memory Sticks as manufactured by Sony Corporation,

	EEPROM, flash memory, hard disk, or the like. The memory can store any of a number of pieces or amount of information and data used by the mobile device to implement the functions of the mobile station. For example, the memory can store an identifier, such as an international mobile equipment identification (IMEI) code, international mobile subscriber identification (IMSI) code, mobile device integrated services digital network (MSISDN) code, or the like, capable of uniquely identifying the mobile device. The memory can also store content. The memory may, for example, store computer program code for an application and other computer programs. For example, in one embodiment of the invention, the memory may store computer program code for performing any combination of Steps **106-109** of **FIG. 1** discussed above. In particular, the memory may store computer program code for receiving a policy update script including one or more modifications to the security policy and for processing the policy update script using an OSGi policy update resource processor **317**, also included in the electronic device, in order to effect the modifications to the security policy. In general, the OSGi policy update resource processor **317** is a software component that is capable of handing the life cycle of a particular resource type by processing the resource to create artifacts that are then removed when the resource is dropped. **[0054]** Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these exemplary embodiments of the invention pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that exemplary embodiments of the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation. **Aarnos Fig 1.** To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1c] is in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the	Aarnos discloses in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.

service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.	*See, e.g.:* 1. A method of updating a security policy associated with an electronic device, said method comprising: Receiving a policy update script comprising one or more modifications to the security policy; and Processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. 3. The method of claim 2 further comprising: Verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. 5. The method of claim 4, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. 6. The method of claim 5, wherein the modifications further grant one or more existing software components permission to access the new software component. **7**. An electronic device capable of updating a security policy associated with the electronic device, said electronic device comprising: an OSGi policy update resource processor configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **9**. The electronic device of claim 8, wherein the resource processor is further configured to verify the signature in order to determine whether the transmitting party is authorized to modify the security policy. **10**. The electronic device of claim 9, wherein the resource processor is further configured to determine, based at least in part on the signature, an extent to which the transmitting party is authorized to modify the security policy.

	12. The electronic device of claim 10, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device, and wherein the modifications further grant one or more existing software components permission to access the new software component. **13**. An apparatus capable of updating a security policy associated with an electronic device, said apparatus comprising: a processor; and a memory in communication with the processor, said memory storing an application executable by the processor, wherein the application is configured, upon execution, to: generate a policy update script comprising one or more modifications to the security policy, said policy update script capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and transmit the policy update script. **14**. The apparatus of claim 13, wherein the application is further configured, upon execution, to associate a signature with the policy update script, said signature capable of being verified in order to determine whether a party associated with the apparatus is authorized to modify the security policy. **16**. The apparatus of claim 15, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. **17**. The apparatus of claim 16, wherein the modifications further grant one or more existing software components permission to access the new software component. **19**. A system for updating a security policy associated with an electronic device, said system comprising: an apparatus configured to generate a policy update script comprising one or more modifications to the security policy, said apparatus further configured to transmit the policy update script; and

	an electronic device configured to receive the policy update script, said electronic device comprising an OSGi policy update resource processor configured to process the policy update script received in order to effect the modifications to the security policy. **27**. A computer program product for updating a security policy associated with an electronic device, wherein the computer program product comprises at least one computer-readable storage medium having computer-readable program code portions stored therein, said computer-readable program code portions comprising: a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **29**. The computer program product of claim 28, wherein the computer-readable program code portions further comprise: a third executable portion for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. **31**. The computer program product of claim 30, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device. **32**. The computer program product of claim 31, wherein the modifications further grant one or more existing software components permission to access the new software component. **33**. An apparatus for updating a security policy associated with an electronic device, said apparatus comprising: a means for receiving a policy update script comprising one or more modifications to the security policy; and

	a means for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **34**. The apparatus of claim 33, wherein the policy update script further comprises a signature corresponding with a transmitting party from whom the policy update script is received, said apparatus further comprising: a means for verifying the signature in order to determine whether the transmitting party is authorized to modify the security policy. **35**. The apparatus of claim 33 further comprising: a means for receiving a new software component associated with the policy update script; and a means for installing the new software component, wherein the modifications to the security policy grant the new software component permission to access one or more existing software applications installed on the electronic device and one or more existing software components permission to access the new software component. **[0007]** Currently, however, in order to modify the electronic device security policy, a party must have AllPermission, a Java-based permission that grants permission to access everything on the electronic device, or a similar and equally powerful permission. However, manufacturers and, in some instances, network operators are generally the only parties with such a powerful permission. This makes it nearly impossible for any party other than the manufacturer or network operator to modify the existing security policy. **[0008]** A need, therefore, exists for a way for parties not limited to the device manufacturer or network operator to modify the existing security policy of an electronic device after a user has taken possession of the electronic device. **[0009]** In general, exemplary embodiments of the present invention provide an improvement over the known prior art by, among other things, providing a convenient and safe way to update the security policy associated with an electronic device, such as a cellular telephone, personal digital assistant (PDA), personal computer (PC), laptop, pager, television, or the like, or one or more electronic devices operating on a motor vehicle, after a user has purchased the device and taken it away for use. In particular, exemplary embodiments provide a scripting tool that can be used to create a policy update script, or resource application or file, that describes the desired modifications to an electronic

	device security policy. Exemplary embodiments further provide an OSGi resource processor, referred to as a Policy Update Resource Processor, that is located on the electronic device and is configured to carry out the security policy modifications outlined in the policy update script. In particular, in one exemplary embodiment, the modifications may be those necessary to provide a new software component, with which the script corresponds, the requisite permissions to access other software components and resources available on the electronic device. The script may also describe how the security policy should be modified, in turn, to provide the other software components access to the services of the new software component. **[0010]** In accordance with one aspect, a method is provided of updating a security policy associated with an electronic device. In one exemplary embodiment, the method includes: (1) receiving a policy update script comprising one or more modifications to the security policy; and (2) processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0011]** According to another aspect, an electronic device is provided that is capable of updating a security policy associated with the electronic device. In one exemplary embodiment the electronic device includes an OSGi policy update resource processor that is configured to receive a policy update script comprising one or more modifications to the security policy and to process the policy update script received in order to effect the modifications to the security policy. **[0012]** According to yet another aspect, an apparatus is provided that is capable of updating a security policy associated with an electronic device. In one exemplary embodiment, the apparatus includes a processor and a memory in communication with the processor that stores an application executable by the processor, wherein the application is configured, upon execution, to: (1) generate a policy update script comprising one or more modifications to the security policy, wherein the policy update script is capable of being processed by an OSGi policy update resource processor in order to effect the modifications; and (2) transmit the policy update script. **[0013]** In accordance with another aspect, a system is provided for updating a security policy associated with an electronic device. In one exemplary embodiment, the system includes: (1) a network entity configured to generate a policy update script comprising one or more modifications to the security policy and to transmit the policy update script; and (2) an electronic device configured to receive the policy update script, wherein the electronic device comprises an OSGi policy update resource processor that is configured to process the policy update script received in order to effect the modifications to the security policy.

	[0014] In accordance with yet another aspect, a computer program product is provided for updating a security policy associated with an electronic device. The computer program product contains at least one computer-readable storage medium having computer-readable program code portions stored therein. The computer-readable program code portions of one exemplary embodiment include: (1) a first executable portion for receiving a policy update script comprising one or more modifications to the security policy; and (2) a second executable portion for processing the policy update script using an OSGi policy update resource processor in order to effect the modifications to the security policy. **[0022]** Once the software component has been developed, in Step **102**, a policy update script is generated that describes the modifications that must be made to the electronic device security policy in order to enable the new software component to access other services and resources of the electronic device, and vice versa (i.e., the modifications grant the appropriate permissions to the various components). The policy update script may, for example, be in the form of an Extensible Markup Language (XML) file, or the like. **[0023]** The developed software component and the corresponding policy update script are then combined, in Step **103** into a deployment (or installation) package for deployment on the device. The deployer (or party responsible for creating the deployment package and providing it to the electronic device, which may or may not be the software developer), in Step **104** signs the package (i.e., incorporates a digital signature, such as a private key, with the package). The signature will be used to verify whether and to what extent the signer (i.e., the deployer) is authorized to modify the electronic device security policy; thus providing increased security to the policy updating process. In one exemplary embodiment, different parties may be provided with different levels of authorization. For example, where one party may have authorization to make wholesale modifications to the existing security policy, other parties may have only restricted access. **[0025]** Regardless of how the deployment package is received by the electronic device (in Step **106**), upon receipt, installation of the deployment package begins (Step **107**). In one exemplary embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment package is in fact authorized to modify the existing security policy of the mobile device (Step **108**). Assuming the signature is verified and that the deployer is authorized (based on the existing electronic device security policy), in Step **109**, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script.

	[0026] In particular, according to the OSGi specification, a deployment service exists on the electronic device that is configured to process deployment or installation packages received by the electronic device. This deployment service comprises one or more plug-ins called resource processors, wherein different resource processors are capable of processing different installation packages. In particular, resource processors, or software components that may be located on the device itself or within the deployment package to be installed, handle the lifecycle of specific resource types by processing the resource to create artifacts that are then removed when the resource is dropped. The use of a plug-in architecture for the deployment service is beneficial since it enables the use of multiple types of resources in the installation package (i.e., for each new type of resource a new resource processor, or plug-in, can be added where necessary). **[0027]** According to exemplary embodiments of the present invention, a new plug-in or OSGi resource processor, referred to as the Policy Update Resource Processor is included in the deployment service. The Policy Update Resource Processor is configured to recognize the policy update script and to conduct the necessary security policy update according to the script. In one exemplary embodiment, usage of the Policy Update Resource Processor is protected by a new Java 2 permission, such that only deployment packages assigned this new permission can run this new processor. The assignment of the Java 2 permission is carried out based on the signature information of the deployment package. In other words, verifying the signature incorporated with the package in order to determine whether, and to what extent, the signer is authorized to modify the security policy, in essence verifies that the party signing the package has been given the new permission. **[0028]** As mentioned briefly above, exemplary embodiments of the present invention are not limited to situations where a new software component is to be installed on the electronic device. In contrast, the policy update script may be used any time a party desires to modify the existing security policy and is authorized to do so. In one exemplary embodiment, rather than including the policy update script in a deployment package for a new software component, a manufacturer or operator may create an "empty" deployment or installation package containing only the policy update script (thus eliminating Step 101). The manufacturer or operator could then provide the package to the appropriate parties, such as the software developer. Using this technique, manufacturers and operators would no longer be required to run the actual installation or remote policy management themselves. The below exemplary use case provides an example of where an empty deployment package may be used. **[0037]** The MSC **16** can be coupled to a data network, such as a local area network (LAN), a metropolitan area network (MAN), and/or a wide area network (WAN). The MSC can be directly coupled to the data network. In one typical embodiment, however, the MSC is coupled to a Packet

	Control Function (PCF) **18**, and the PCF is coupled to a Packet Data Serving Node (PDSN) **19**, which is in turn coupled to a WAN, such as the Internet **20**. In turn, devices such as processing elements (e.g., personal computers, server computers or the like) can be coupled to the mobile station **10** via the Internet. For example, the processing elements can include devices corresponding with an Authorized Policy Administrator **22** (i.e., a party having authorization to create policy update scripts that will be read by a Policy Update Resource Processor on the mobile station in order to modify the existing security policy) and/or a Software Developer **24**, discussed above. As will be appreciated, the processing elements can comprise any of a number of processing devices, systems or the like capable of operating in accordance with embodiments of the invention. **[0040]** One or more mobile stations **10** (as well as one or more processing elements, although not shown as such in FIG. 2) can further be coupled to one or more wireless access points (APs) **36**. The AP's can be configured to communicate with the mobile station in accordance with techniques such as, for example, radio frequency (RF), Bluetooth (BT), infrared (IrDA) or any of a number of different wireless networking techniques, including WLAN techniques. The APs may be coupled to the Internet **20**. Like with the MSC **16**, the AP's can be directly coupled to the Internet. In one embodiment, however, the APs are indirectly coupled to the Internet via a GTW **28**. As will be appreciated, by directly or indirectly connecting the mobile stations and the processing elements (e.g., devices associated with the Authorized Policy Administrator **22** and/or Software Developer **24**) and/or any of a number of other devices to the Internet, whether via the AP's or the mobile network(s), the mobile stations and processing elements can communicate with one another to thereby carry out various functions of the respective entities, such as to transmit and/or receive data, content or the like. As used herein, the terms “data,” “content,” “information,” and similar terms may be used interchangeably to refer to data capable of being transmitted, received and/or stored in accordance with embodiments of the invention. Thus, use of any such terms should not be taken to limit the spirit and scope of embodiments of the invention. **[0048]** The mobile station can also include means, such as memory including, for example, a subscriber identity module (SIM) **320**, a removable user identity module (R-UIM) (not shown), or the like, which typically stores information elements related to a mobile subscriber. In addition to the SIM, the mobile device can include other memory. In this regard, the mobile station can include volatile memory **322**, as well as other non-volatile memory **324**, which can be embedded and/or may be removable. For example, the other non-volatile memory may be embedded or removable multimedia memory cards (MMCs), Memory Sticks as manufactured by Sony Corporation, EEPROM, flash memory, hard disk, or the like. The memory can store any of a number of pieces or amount of information and data used by the mobile device to implement the functions of the mobile

	station. For example, the memory can store an identifier, such as an international mobile equipment identification (IMEI) code, international mobile subscriber identification (IMSI) code, mobile device integrated services digital network (MSISDN) code, or the like, capable of uniquely identifying the mobile device. The memory can also store content. The memory may, for example, store computer program code for an application and other computer programs. For example, in one embodiment of the invention, the memory may store computer program code for performing any combination of Steps **106-109** of **FIG. 1** discussed above. In particular, the memory may store computer program code for receiving a policy update script including one or more modifications to the security policy and for processing the policy update script using an OSGi policy update resource processor **317**, also included in the electronic device, in order to effect the modifications to the security policy. In general, the OSGi policy update resource processor **317** is a software component that is capable of handing the life cycle of a particular resource type by processing the resource to create artifacts that are then removed when the resource is dropped. **[0054]** Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these exemplary embodiments of the invention pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that exemplary embodiments of the inventions are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[2] The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control.	Aarnos discloses the method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 2. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it

	would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[3] The method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).	Aarnos discloses the method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN). *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 3. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[4] The method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network.	Aarnos discloses the method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 4. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[5] The method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.	Aarnos discloses the method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 5. *See supra* claim 1.

	To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[6] The method of claim 1, further comprising:	Aarnos discloses the method of claim 1. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 6. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[6a] obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and	Aarnos discloses obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 6. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[6b] based on the service usage measure, taking an action.	Aarnos discloses based on the service usage measure, taking an action. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 6. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

[7] The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity.	Aarnos discloses the method of claim 6, wherein the service usage measure comprises a measure of a service usage activity. *See supra* claims 1 and 6. In addition, Aarnos anticipates and/or renders obvious claim 7. *See supra* claims 1 and 6. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[8] The method of claim 6, wherein the action is to verify the service usage measure.	Aarnos discloses the method of claim 6, wherein the action is to verify the service usage measure. *See supra* claims 1 and 6. In addition, Aarnos anticipates and/or renders obvious claim 8. *See supra* claims 1 and 6. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[9] The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device.	Aarnos discloses the method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device. *See supra* claims 1 and 6. In addition, Aarnos anticipates and/or renders obvious claim 9. *See supra* claims 1 and 6. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[12] The method of claim 1, wherein the configuration information	Aarnos discloses the method of claim 1, wherein the configuration information comprises at least a portion of the service profile. *See supra* claim 1.

comprises at least a portion of the service profile.	In addition, Aarnos anticipates and/or renders obvious claim 12. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[13] The method of claim 1, wherein the service control link is secured by an encryption protocol.	Aarnos discloses the method of claim 1, wherein the service control link is secured by an encryption protocol. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 13. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[14] The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.	Aarnos discloses the method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 14. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[16] The method of claim 1, wherein the device service state comprises information associated with an encryption key.	Aarnos discloses the method of claim 1, wherein the device service state comprises information associated with an encryption key. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 16. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it

	would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[17] The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.	Aarnos discloses the method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 17. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[18] The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.	Aarnos discloses the method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state. *See supra* claim 1. In addition, Aarnos anticipates and/or renders obvious claim 18. *See supra* claim 1. To the extent Aarnos does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Aarnos alone or it would have been obvious to combine Aarnos with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.